The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
3/9/2010
3/11/2010 - UPDATED

SUBJECT:
Vulnerability in Internet Explorer Could Allow Remote Code Execution

ORIGINAL OVERVIEW:
A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. **At this point in time, no patches are available for this vulnerability**. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

March 11 - UPDATED OVERVIEW:
Exploit code is publicly available. The exploit code has also been added to the Metasploit exploitation framework. Availability of this exploit will increase the chance of exploitation of this vulnerability. We have tested the exploit code in our lab, and confirmed that the exploit works with Internet Explorer 6 and Internet Explorer 7 and allows for remote code execution.

SYSTEMS AFFECTED:

- Windows 2000
- Windows XP
- Windows Vista
- Windows Server 2008
- Internet Explorer 6
- Internet Explorer 7

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

ORIGINAL DESCRIPTION:
A vulnerability has been identified in Microsoft Internet Explorer that could allow an attacker to take complete control of an affected system. The vulnerability exists due to an invalid pointer reference being used within Internet Explorer. It is possible, under certain conditions, for the invalid pointer to be accessed after an object is deleted. An attacker can exploit this vulnerability by hosting a specially crafted webpage. Once the user visits the page, the vulnerability will allow Internet Explorer to access a freed object which could allow remote code execution.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Please note: At this time, Microsoft has not provided a patch, and is aware of targeted attacks attempting to exploit this vulnerability.

March 11 - UPDATED DESCRIPTION:
Exploit code is publicly available. The exploit code has also been added to the Metasploit exploitation framework. Availability of this exploit will increase the chance of exploitation of this vulnerability. We have tested the exploit code in our lab, and confirmed that the exploit works with Internet Explorer 6 and Internet Explorer 7 and allows for remote code execution.

RECOMMENDATIONS:
The following actions should be taken:
· Install the appropriate Microsoft patch as soon as it becomes available after appropriate testing.
· Consider upgrading to Internet Explorer 8 since according to Microsoft it is currently not affected.
· Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
· If your organization has deployed alternate browsers, recommend staff utilize an alternate browser.
· Consider implementing the following workarounds provided by Microsoft:
1. Enable DEP for Internet Explorer 6 Service Pack 2 or Internet Explorer 7
2. Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones
3. Modify the Access Control List (ACL) on iepeers.dll
4. Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone

ORIGINAL REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/advisory/981374.mspx

Secunia:
http://secunia.com/advisories/38860/

SecurityFocus:
http://www.securityfocus.com/bid/38615

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806

UPDATED REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/advisory/981374.mspx

US-CERT
http://www.kb.cert.org/vuls/id/744549

SecurityFocus:
http://www.securityfocus.com/bid/38615